Vysoké učení technické v Brně

Fakulta informačních technologií

Síťové aplikace a správa sítí

2019/2020

Programování síťové služby

Varianta: Whois tazatel

Juraj Lazorík (xlazor02)

Brno, 18. novembra 2019

Obsah

1. Zadanie

Naštudujte si problematiku geolokácie IP adresy a preniknite do detailov protokolu WHOIS, zoznámte sa so službou DNS. Implementujte program, ktorý bude k vloženému hostname/IP adrese zobrazovať maximum informácií dostupných k danému záznamu práve z WHOIS.

2. Úvod

Whois tazatel je aplikácia ktorá pozostáva z dvoch častí. Prvá časť získava DNS záznamy z vloženej IP adresy alebo hostname. Druhá časť získava WHOIS záznamy pre vloženú adresu a to zo serveru, ktorý opäť zadá uživateľ, a to vo forme IP adresy alebo hostname.

2.1. DNS záznamy

DNS záznamy obsahujú informácie o každej webovej stránke na internete. Základné typy, s ktorými budeme pracovať sú: A, AAAA, MX, NS, SOA, PTR, CNAME.

A - Najzákladnejší typ záznamu. Používa sa na nasmerovanie domény alebo subdomény na IPv4 adresu.

AAAA - Tento záznam je rovnaký ako záznam A, ale umožňuje nasmerovať doménu alebo subdomény na adresu IPv6.

MX - Záznam určuje, kam majú smerovať e-maily, ak sa odosielajú na adresu danej domény.

NS - Name Server záznam udáva, ktorý DNS server je autoritatívny pre doménu, a teda server, ktorý obsahuje skutočné záznamy DNS.

SOA - Start of Authority alebo teda záznam začiatku autority je typ záznamu, ktorý obsahuje administratívne informácie o zónach a najmä pokiaľ ide o zóny prenosu.

PTR - Tento záznam slúži na zistenie, či je daná IP adresa pripojená k nejakému hostname alebo doméne. Používa sa na spätné vyhľadávanie DNS(reverse lookup).

CNAME - Záznam sa používa namiesto záznamu A, ak je doména alebo subdoména aliasom inej domény.

2.2. WHOIS záznamy

WHOIS je databáza, ktorá slúži k evidencii údajov o majiteľoch internetových domén a IP adries. V jednotlivých záznamoch budeme vyhľadávať tieto záznamy: inetnum, inet6num, netname, descr, country, address, phone, admin-c.

Inetnum - Rozsah IPv4 adries, ktoré popisuje nájdený objekt.

Inet6num - Rozsah IPv6 adries, ktoré popisuje nájdený objekt.

Netname - Názov rozsahu IP adries.

Descr - Popis objektu, ktorému patrí adresový priestor v inetnum.

Country, address, phone, admin-c, person - Krajina, adresa, telefón, správca objektu.

3. Spustenie programu

Projekt rozbalíme z archívu tar. Následne potrebujeme vytvoriť spustiteľný súbor. Ten vytvoríme pomocou príkazu `make`, ktorý preloží zdrojový súbor `isa-tazatel.c`. V prípade, že spustiteľný súbor chceme odstrániť, použijeme príkaz `make clean`, ktorý súbor vymaže. Program spustíme následovne:

```
$ ./isa-tazatel [ -w IP|hostname WHOIS serveru ] [ -q
IP|hostname ]
```

Oba argumenty sú povinné. Argumenty môžu byť zadané v ľubovoľnom poradí. Po oboch prepínačoch musí nasledovať odpovedajúci argument. Zvislá čiara medzi argumentami znamená, že sa môže zvoliť len jeden z nich.

3.1. Argumenty:

`-w IP|hostname WHOIS serveru`: Povinný argument, ktorý označuje WHOIS server na ktorý sa budeme pripájať. Validné hodnoty argumentu sú IPv4, IPv6 alebo hostname.

`-q IP|hostname`: Povinný argument, ktorý označuje, pre ktorú adresu či hostname budeme hľadať odpovedajúce záznamy. Validné hodnoty argumentu sú IPv4, IPv6 alebo hostname.

3.2. Príklad spustenia programu:

```
$ ./isa-tazatel -w whois.ripe.net -q www.fit.vutbr.cz

$ ./isa-tazatel -q www.fit.vutbr.cz -w whois.ripe.net

$ ./isa-tazatel -q 147.229.9.23 -w 193.0.6.135

$ ./isa-tazatel -q 2001:67c:1220:809::93e5:917 -w
193.0.6.135

$ ./isa-tazatel -q www.fit.vutbr.cz -w
2001:67c:2e8:22::c100:687
```

4. Návrh riešenia

Program isa-tazatel sme implementovali v jazyku C.

4.1. Spracovanie argumentov

Ako prvé, po spustení programu spracujeme argumenty. Kontrolu argumentov vykonávame za pomoci funkcie `getopt`. Každý argument následne uložíme do premennej, s ktorou budeme pracovať. V prípade zle zadaných argumentov vypíšeme príslušnú chybovú hlášku a poskytneme vzorový príklad na spustenie.

4.2. DNS

V programe sa najprv zaoberáme DNS časťou. Pre získanie DNS záznamu potrebujeme hostname. Funkciou `isValidIpAddressOrHost` zistíme, či sme od uživateľa dostali IPv4 adresu IPv6 adresu alebo hostname. S IP adresami nemôžeme priamo pracovať a v tomto prípade si musíme zaobstarať hostname patriaci k danej IP. To urobíme pomocou funkcie `IPtoHostName` pre IPv4 a `IPtoHostName6` pre IPv6. Tieto funkcie využívajú metódu `getnameinfo`. Teraz môžeme začať získavať jednotlivé DNS záznamy. Pomocou metódy `res_query` získavame záznamy A, AAAA, MX, NS, SOA, PTR, CNAME. Náročnejšou úlohou je spracovanie záznamov. To vykonávame pomocou funkcií z knižnice na prácu so stringami. Ak daný záznam získame tak ho vypíšeme, ak nie program nás upozorní, že záznam chýba. V prípade záznamu PTR ak záznam nenájdeme, využijeme to, že na získavanie DNS záznamu už vopred potrebujeme hostname. Ten vypíšeme, ak uživateľ zadal IP adresu. Ako DNS resolver využívame ten, ktorý je zadaný v operačnom systéme.

4.3. WHOIS

V časti WHOIS je to opačne. Na pripojenie k serveru potrebujeme získať IP adresu. V prípade, že uživateľ zadal WHOIS ako hostname, tak ho prevedieme na IP adresu pomocou funkcie `hostname_to_ip`. Ďalej si na vytvorenie pripojenia k serveru potrebujeme vytvoriť socket. Ten vytvárame rôzne, a to na základe toho, či sa budeme pripájať pomocou IPv4 alebo IPv6. Nasleduje samotné vytvorenie spojenia. Ak je spojenie úspešne vytvorené odošleme na server správu, ktorá obsahuje hodnotu za argumentom -q a teda IP alebo hostname, ktorý zadal uživateľ. Pri úspechu nám server odošle všetky informácie, ktoré má k danej adrese. Z tých vyberieme tie, ktoré požadujeme a teda inetnum, inet6num, netname, descr, country, address, phone, admin-c. Ak žiadne z týchto informácií nenájdeme, program vypíše hlášku, že nenašiel žiadne dáta.

4.3.1. Rekurzívne dotazovanie

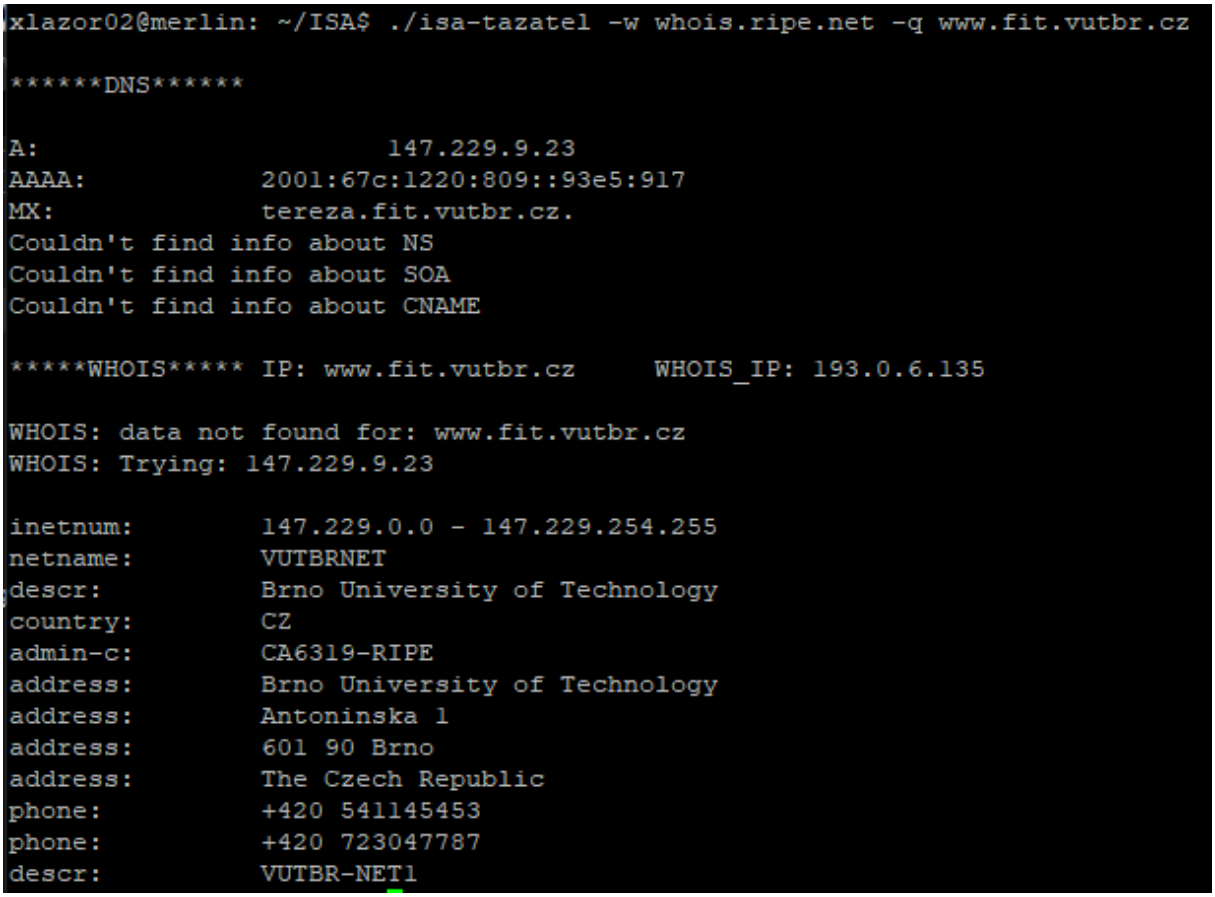
V prípade, ak server odošle chybu `ERROR:101`, rekurzívne zavoláme funkciu obsluhujúcu pripojenie sa k serveru `whois_query` a správu, ktorú odosielame na server pozmeníme. Ak v pôvodnej správe bola IP adresa, tak v novej správe pošleme hostname patriaci k príslušnej IP adrese. Ak bol v pôvodnej správe hostname, tak v novej správe pošleme IP adresu prislúchajúcu k danému hostname. Na túto zmenu uživateľa vždy upozorníme. Ak sa nám nepodarí prevod z IP adresy na hostname a naopak, tak uživateľa opäť na túto skutočnosť upozorníme.

5. Testovanie

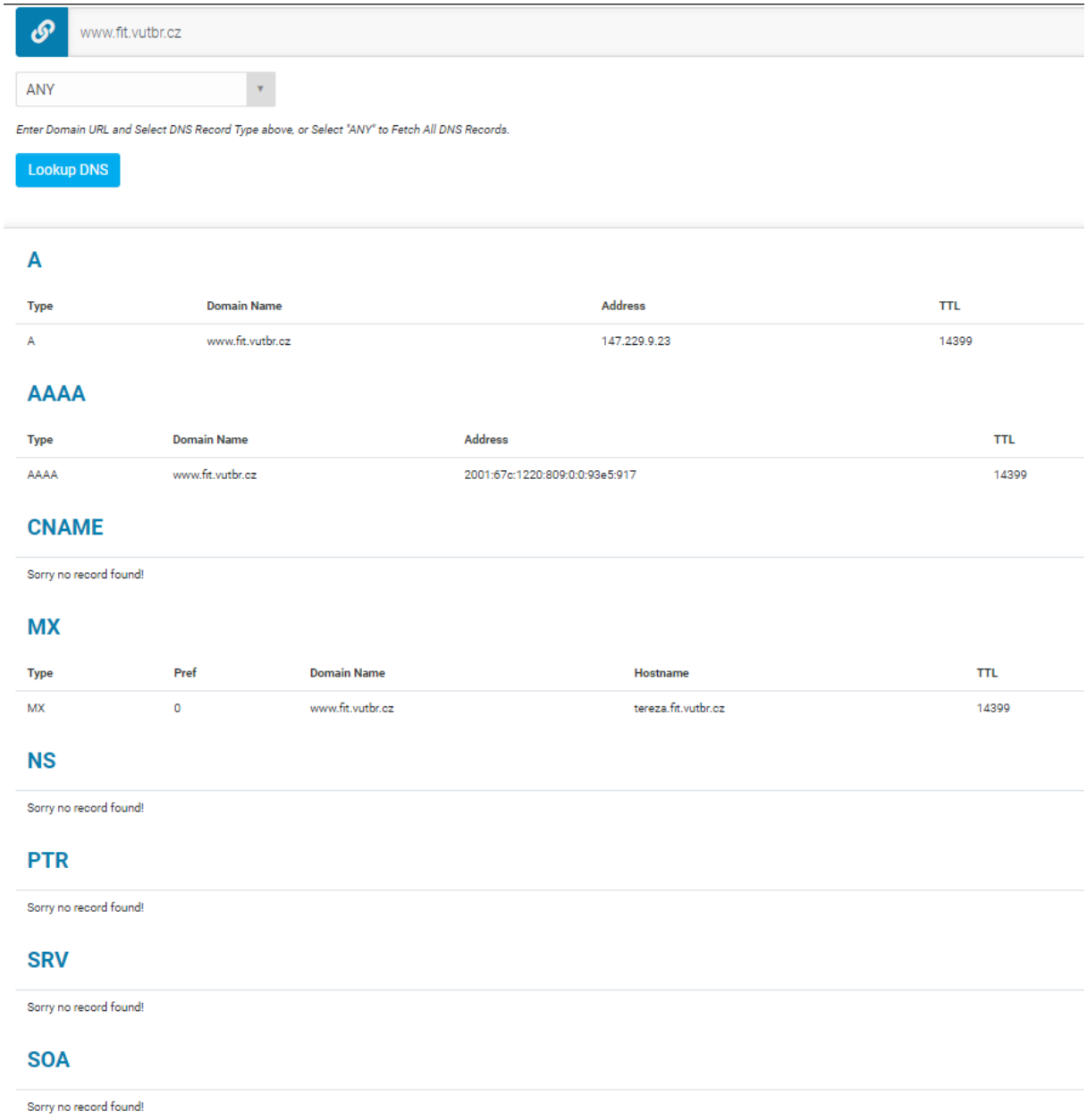
Program bol testovaný na virtuálnom stroji, ktorý bol vytvorený z poskytnutého referenčného Linux obrazu. Taktiež bol testovaný na virtuálnom stroji Merlin, kde boli výsledky rovnaké ako na referenčnom Linuxe. Pre prehľadnosť budeme v tomto manuáli pracovať s virtuálnym strojom Merlin.

Na porovnanie výsledkov testovania budeme používať:

- Pre DNS: https://dnschecker.org/all-dns-records-of-domain.php
- Pre WHOIS: http://whois.domaintools.com/ a https://www.ripe.net/



Obrázok 1 - Výsledok nášho programu



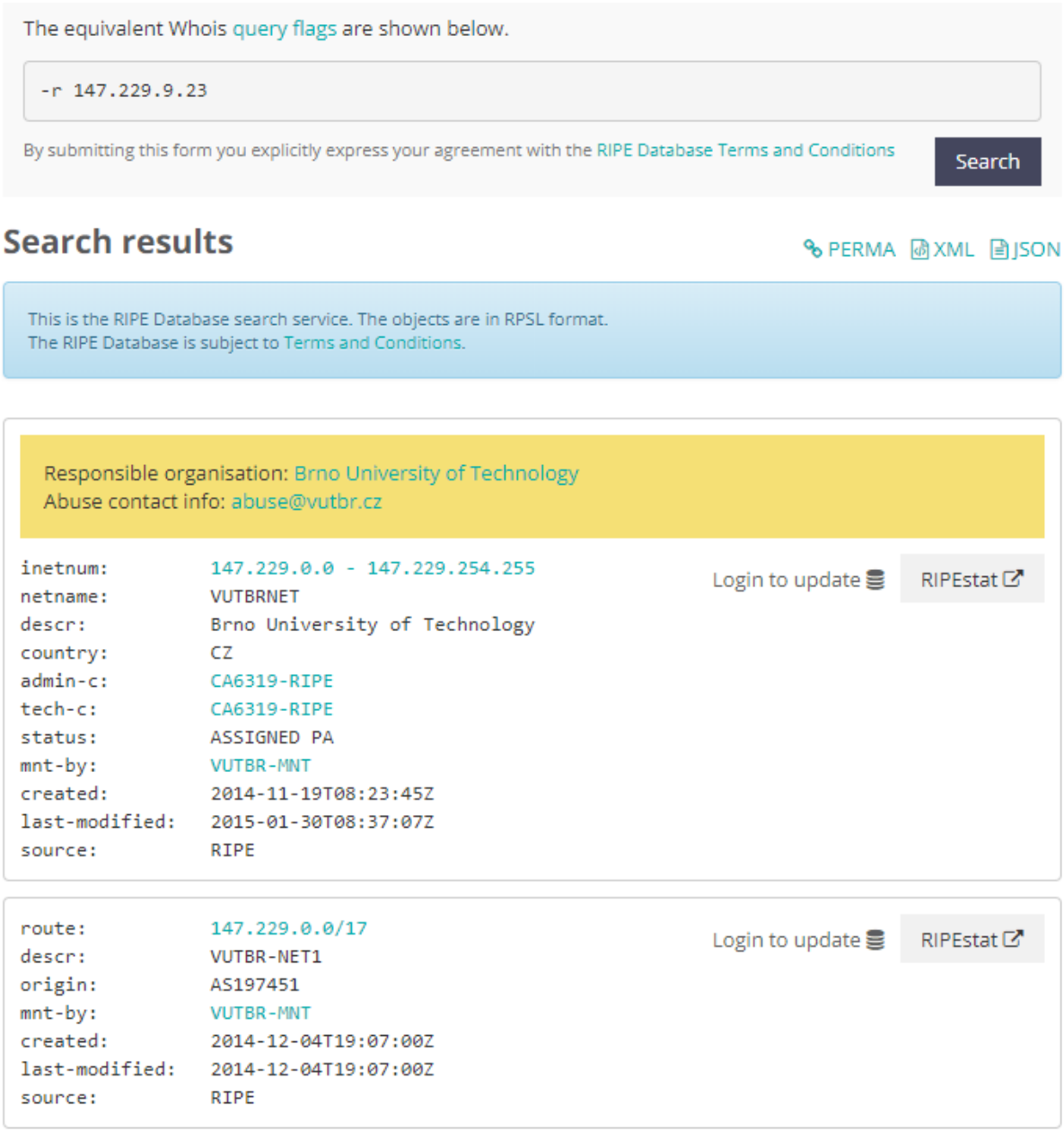
Obrázok 2 - Výsledok stránky DNSchecker

Whois Record (last updated on 2019-11-18)

```
domain:       vutbr.cz
registrant:   SB:VUTBR-CZ
admin-c:      VUTBR-TPODER
admin-c:      CID:IHAZMUK
nsset:        NSS:VUTBR:1
keyset:       KEYSET-VUTBR.CZ:1
registrar:    REG-INTERNET-CZ
registered:   19.05.1994 02:00:00
changed:      05.02.2019 10:36:30
expire:       12.10.2023

contact:      SB:VUTBR-CZ
org:          Vysoke uceni technicke v Brne
name:         Vysoke uceni technicke v Brne
address:      Antoninska 548/1
address:      Brno
address:      601 90
address:      CZ
registrar:    REG-INTERNET-CZ
created:      10.08.2001 22:13:00
changed:      15.05.2018 21:32:00

contact:      VUTBR-TPODER
org:          Vysoké učení technické v Brně
name:         Tomáš Podermański
address:      Antonínská 548/1
address:      Brno
address:      601 90
address:      Jihomoravský kraj
address:      CZ
registrar:    REG-INTERNET-CZ
created:      05.02.2019 10:32:19

contact:      CID:IHAZMUK
org:          Vysoké učení technické v Brně
name:         Ivo Ha\u017emuk
address:      Antonínská 548/1
address:      Brno
address:      601 90
address:      Jihomoravský kraj
address:      CZ
registrar:    REG-INTERNET-CZ
created:      06.10.2008 17:30:01
changed:      05.08.2019 11:24:03

nsset:        NSS:VUTBR:1
nserver:      rhino.cis.vutbr.cz (147.229.3.10, 2001:67c:1220:e000::93e5:30a)
nserver:      pipit.cis.vutbr.cz (77.93.219.110, 2a01:430:120::4d5d:db6e)
tech-c:       CID:IHAZMUK
tech-c:       VUTBR-TPODER
registrar:    REG-INTERNET-CZ
created:      14.10.2008 11:03:11
changed:      05.02.2019 10:45:05

keyset:       KEYSET-VUTBR.CZ:1
dnskey:       257 3 5
AwEAAfhR+s/4SLZZNA+kD2u1UgYBUu+X3Avi60QCaE1o2STterM405s8mWMWJOlZGtjjIky3TEMxQ0+ZtMbEeJu2wNDL
dV/XglX+pJAjyy728WJH4u2/gJR8ZWsEIc0Jwb4FjwmBiF2Koz0SGVvrzEZ9T1H7dHq2X6f8KzYBotJyrAIWr9tZi/9t
HrngZJ5wXELmMPWCfEFapdQMoKWoNvzrMYFli17RMz7gJzCmNxMRV8/WkjsNPgYsTKpsAT8qEsXiTN9987AIKPHvc5j+
/njq+fTXdOqGVpIgSiso+qJMddEMBcu/MBBYVFOwRQe1ez2tMwIX7y5mwDvK0wsmyRvHugfFuxSnfiJvQr05kSnj0wxD
9s9LNhrF4PocrcYqnBN/lBx9D6633jJ3zT3T5Foe/Vj9A/X7F2oN6FOkdwO+YSEUot980pJQut6DR22UP4bLakyDMiTd
OQ31c/dRIoTsccxw+838pXFyEPgiqOHRSeN/w9km6BIDcl+32Xq97kXSMQH6AxOUsx9/Mxdj7ISwbS4utaAWoP460+TM
cnfJfWfBNEWhuFvnfB9l63ZjZToB2PUVhrTxRwKUlfMLegSJKoZfiae82kK1pN4xFYyquKSykm/oXsM2w4OQvpqGcTwA
XzZ5s95J45f7PsCap0bscGKumxsHcDswWpUz/UVosIrr
tech-c:       CID:IHAZMUK
tech-c:       VUTBR-TPODER
registrar:    REG-INTERNET-CZ
created:      13.10.2008 10:27:37
changed:      14.02.2019 13:36:06
```

Obrázok 3 - Výsledok stránky whois.domaintools

Testovanie ukázalo, že výsledky DNS sú správne. WHOIS výsledky sú odlišné, pretože v našom programe sa dotazujeme len na WHOIS server zadaný užívateľom a nehľadáme a nepožívame ten najvhodnejší. Ak použijeme internetový nastroj, ktorý pracuje len s našim serverom dostaneme výsledky, ktoré sa budú viac podobať naším. Skúsme teda porovnávať naše výsledky so stránkou https://www.ripe.net/.



Obrázok 4 - Výsledok stránky ripe

Tu už môžeme pozorovať že výsledky sú skutočne podobné výsledkom našej aplikácie.

6. Zdroje

1. WHOIS. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-11-18]. Dostupné z: https://en.wikipedia.org/wiki/WHOIS

2. DNS Management: Record Types And When To Use Them. Pressable [online]. Pressable, 2011- [cit. 2019-11-18]. Dostupné z: https://kb.pressable.com/article/dns-record-types-explained/

3. What Is A DNS CNAME Record? Cloudflare [online]. San Francisco: Cloudflare, 2019 [cit. 2019-11-18]. Dostupné z: https://www.cloudflare.com/learning/dns/dns-records/dns-cname-record/

4. Inetnum: Object Template. *Apnic* [online]. South Brisbane: Apnic, 2019 [cit. 2019-11-18]. Dostupné z: https://www.apnic.net/manage-ip/using-whois/guide/inetnum/

5. RIPE Database Query. *Ripe* [online]. Ripe, 2019 [cit. 2019-11-18]. Dostupné z: https://apps.db.ripe.net/db-web-ui/#/query?bflag=false&dflag=false&rflag=true&searchtext=147.229.9.23&source=RIPE

6. DNS Lookup. *DNSCHECKER* [online]. Ripe, 2019 [cit. 2019-11-18]. Dostupné z: https://dnschecker.org/all-dns-records-of-domain.php

7. Whois Record for VutBr.cz. *DOMAINTOOLS* [online]. DOMAINTOOLS, 2019 [cit. 2019-11-18]. Dostupné z: http://whois.domaintools.com/vutbr.cz